Applied Modern Algebra (Spring 2020) Midterm Review Problems

Note: The following sample of practice problems is to help give you an idea of the kinds of questions that might be on the exam. It is not meant to be an exhaustive review of topic that could appear on the exam.

- 1. True or False: $\mathbb{Z}/4\mathbb{Z}$ is a ring. Briefly explain.
- 2. True or False: $\mathbb{Z}/4\mathbb{Z}$ is a field. Briefly explain.
- 3. Let G be a finite group and $a \in G$. What does it mean to say that n is the order of a? What facts do you know about the order of a?
- 4. Write the decimal number 23 in binary.
- 5. Encrypt the string AB using an affine cipher with encryption key (a, b) = (3, 2). Find the decryption key (c, d) associated to (a, b) (i.e., so that encryption with (c, d) is the inverse of encryption with (a, b)).
- 6. Determine, with proof, the number of valid keys for an affine cipher (i.e., the number of keys so that encryption is an invertible process).
- 7. Does performing two affine ciphers (with different keys) provide more security than a single affine cipher? Explain.
- 8. In 1–2 paragraphs, briefly explain how to use frequency analysis to break a Vigenère cipher.
- 9. Find an inverse of 4 mod 101 in two different ways.
- 10. Let p be a prime number. Prove that, for any integer a, we have $a \equiv a^p \mod p$.
- 11. Write a python3 function shiftletter(c,k) which takes in an uppercase alphabetic character (string of length 1) c and an integer k, and returns the character resulting from a cyclic shift of c by k positions. E.g., shiftletter('Z', 1) should return 'A'.
- 12. Write a python3 function isprime(n) which takes in a positive integer n, and returns True if n is prime and False if n is not prime. (Do not worry about efficiency.)